future internet

Review

A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues

Panagiotis Gkonis [1,*], Anastasios Giannopoulos [2], Panagiotis Trakadas [2], Xavi Masip-Bruin [3] and Francesco D'Andria [4]

[1] Department of Digital Industry Technologies, National and Kapodistrian University of Athens, Dirfies Messapies, 34400 Evia, Greece
[2] Department of Port Management and Shipping, National and Kapodistrian University of Athens, Dirfies Messapies, 34400 Evia, Greece; angianno@uoa.gr (A.G.); ptrakadas@pms.uoa.gr (P.T.)
[3] CRAAX Lab, Universitat Politècnica de Catalunya (UPC), 08800 Vilanova i la Geltrú, Spain; xavier.masip@upc.edu
[4] Eviden, BDS INN R&D (Formerly Called ATOS), 08800 Barcelona, Spain; francesco.dandria@eviden.com
* Correspondence: pgkonis@uoa.gr

Abstract: The rapid growth in the number of interconnected devices on the Internet (referred to as the Internet of Things—IoT), along with the huge volume of data that are exchanged and processed, has created a new landscape in network design and operation. Due to the limited battery size and computational capabilities of IoT nodes, data processing usually takes place on external devices. Since latency minimization is a key concept in modern-era networks, edge servers that are in close proximity to IoT nodes gather and process related data, while in some cases data offloading in the cloud might have to take place. The interconnection of a vast number of heterogeneous IoT devices with the edge servers and the cloud, where the IoT, edge, and cloud converge to form a computing continuum, is also known as the IoT-edge-cloud (IEC) continuum. Several key challenges are associated with this new computing systems' architectural approach, including (i) the design of connection and programming protocols aimed at properly manipulating a huge number of heterogeneous devices over diverse infrastructures; (ii) the design of efficient task offloading algorithms aimed at optimizing services execution; (iii) the support for security and privacy enhancements during data transfer to deal with the existent and even unforeseen attacks and threats landscape; (iv) scalability, flexibility, and reliability guarantees to face the expected mobility for IoT systems; and (v) the design of optimal resource allocation mechanisms to make the most out of the available resources. These challenges will become even more significant towards the new era of sixth-generation (6G) networks, which will be based on the integration of various cutting-edge heterogeneous technologies. Therefore, the goal of this survey paper is to present all recent developments in the field of IEC continuum systems, with respect to the aforementioned deployment challenges. In the same context, potential limitations and future challenges are highlighted as well. Finally, indicative use cases are also presented from an IEC continuum perspective.

Keywords: IoT; cloud-based operating systems; edge computing; machine learning; federated learning; task offloading; security and privacy; blockchain technology

check for updates

Citation: Gkonis, P.; Giannopoulos, A.; Trakadas, P.; Masip-Bruin, X.; D'Andria, F. A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues. *Future Internet* **2023**, *15*, 383. https://doi.org/10.3390/fi15120383

Academic Editor: Ping Wang

Received: 7 November 2023
Revised: 21 November 2023
Accepted: 24 November 2023
Published: 28 November 2023

1. Introduction

The unstoppable proliferation of novel computing and sensing device technologies, and the ever-growing demand for data-intensive applications in the edge and cloud, are driving the next wave of transformation in computing systems architecture [1,2]. In the same context, there is a vast number of devices that can collect, process, and transmit data to other devices and systems over the Internet or other communications networks. This new concept, known as the Internet of Things (IoT), enables the collection of data from various and diverse sources in the physical world [3]. Leveraging this concept, many different advanced human-centric services and applications can be widely deployed, such as energy management in smart home environments, remote health monitoring, intelligent transportation, etc. [4].

Since most data are created at the edge, and computationally intensive data processing usually takes place in centralized cloud infrastructures, a flexible interconnection of all involved entities is required to bring the edge as close to the cloud as possible and vice versa. Together with the cloud, edge-based computing is pushing the limits of the traditional centralized cloud computing solutions enabling, among other features, efficient data processing and storage as well as low latency for service execution. In this context, multi-access edge computing (MEC), formerly mobile edge computing, is a new architectural concept that enables cloud computing capabilities and an IT service environment at the edge of any network [5,6]. Located in close proximity to the end users and connected IoT devices, MEC provides extremely low latency and high bandwidth while always enabling applications to leverage cloud capabilities if necessary. The resulting paradigm shift in computing is centered around the dynamic, intelligent, and yet seamless interconnection of IoT devices, edge, and cloud resources in one computing system to form what is known as a continuum [7,8]. The goal of this synergy is the provision of advanced services and applications to the end users, which is also leveraged by similar advances in the networking field, such as network function virtualization (NFV) [9,10], which decouples network operations from specific hardware equipment, as well as software defined networking (SDN) [11], which enables a holistic and intelligent network management approach.

A continuum, today also referred to as cloud, IoT, edge-to-cloud, or fog-to-cloud continuum, is expected to provide high computational capabilities for data processing at both edge and cloud while inferring and persisting important information for post-mortem and offline analysis. Throughout the rest of this paper, the term continuum will be used to indicate the IoT-edge-cloud (IEC) continuum, unless otherwise stated. The full deployment of such a continuum is expected to leverage the support of latency-critical applications via dynamic task offloading among the IoT nodes and edge or cloud servers. Moreover, data collected directly from all entities of the continuum can be used for optimum resource allocation and scheduling policies [12]. However, there are many technical challenges associated with this new architectural approach:

- Unlike centrally managed clouds, massively heterogeneous systems in the continuum (including IoT devices, edge devices, and cloud infrastructures) are significantly more complex to manage. Furthermore, distributed data management raises an additional level of complexity by classifying data infrastructures, collecting vast and diverse data volumes, providing transparent data access methods, optimizing the internal data flow, and effectively preserving data collections [13].
- Because of the heterogeneity of the involved devices and associated technologies, hardware and technology-agnostic protocols are important, not only to manipulate a large number of interconnected entities but also to enable scalability which is a key concept in the IEC continuum.
- The continuum needs to be effectively managed to optimally meet the application demands during service execution, taking into account multiple constraints, such as the location of the involved nodes (edge or IoT), their transmission and processing capabilities, as well as their energy footprint. Optimum resource allocation in multi-node heterogeneous environments might lead to highly non-convex problems. In this context, machine learning (ML) algorithms have emerged as a promising approach that can solve various optimization problems providing near-optimal solutions [14,15]. In traditional centralized ML approaches, all collected data are sent to a high-performance computing node for proper model training and inference. However, on one hand, the collection of heterogeneous data from all involved nodes of the continuum might increase the pre-processing load, and on the other hand, centralized ML training might jeopardize latency requirements in critical applications. Therefore, as will also be

described in Section 2, the support of distributed and decentralized ML approaches is a key concept in IEC systems [16–18].

- Due to the distributed and dynamic nature of the continuum, with plenty of devices from different owners and provenance, the application of reliability and trustiness becomes fundamentally challenging. Secure mechanisms for accessing the distributed nodes, preserving data privacy, and providing open and transparent operation are fundamental to enhancing trustworthiness [19,20].
- As it was previously mentioned, the continuum puts together a broad and diverse space with multiple heterogeneous devices and protocols. Although there are several standards, open-source projects, and foundations that focus on global communication and management protocols, the envisioned continuum must also consider that some constrained devices will not support any specific tool. Therefore, contributing to an open ecosystem favors interoperability with existing and emerging frameworks, which is a key challenge for next-generation broadband wireless networks [21].

Hence, as it becomes apparent from the above, the optimum design of an IEC infrastructure should address various technical challenges, such as: (i) distributed data management; (ii) continuum infrastructure virtualization and diverse network connectivity; (iii) optimized and scalable service execution and performance; (iv) guaranteed trust, security, and privacy; (v) reliability and trustworthiness; and (vi) support of scalability, extensibility, and adoption of open-source frameworks [22]. These challenges are also depicted in Figure 1. The envisioned effects of edge computing in a wide range of potential use cases, from smart environmental monitoring to future fifth-generation (5G) advanced applications (such as e-health, autonomous driving, smart manufacturing, etc.), have fueled several initiatives aimed at addressing the different challenges posed by the full deployment of an IEC continuum. These challenges become even more important as the discussions on sixth-generation (6G) networks have already started taking place [23,24].

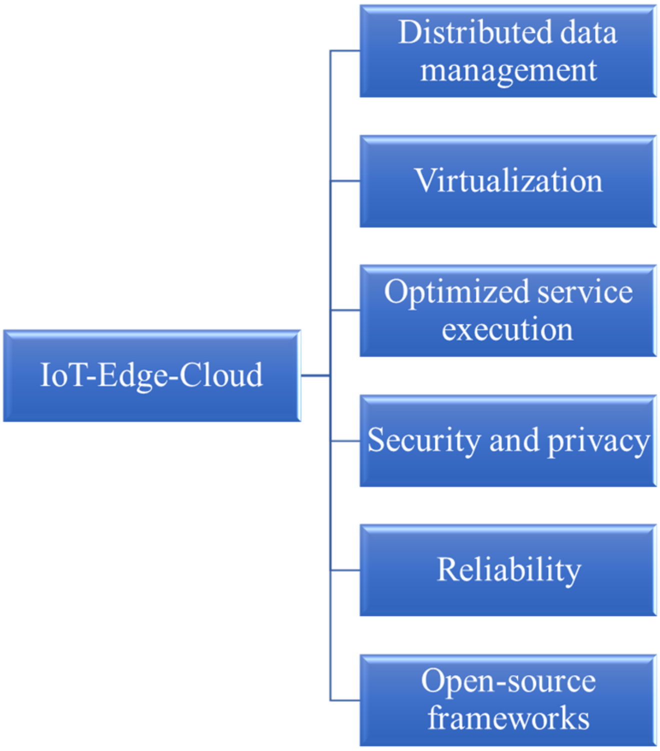

Figure 1. Challenges in the IoT-edge-cloud continuum.

Therefore, the goal of this survey paper is to analyze all recent technological developments in the field of IEC continuum systems. Emphasis will be given on the addressed challenges per case, according to the previous description. In the same context, open issues and limitations will be identified as well. Moreover, potential deployment scenarios based on IEC continuum systems will be also presented. The rest of this survey paper is organized as follows: In Section 1.1 of Section 1, indicative recent survey papers are presented, while the main contributions of our work are highlighted in Section 1.2. In Section 2, the most important supporting technologies in IEC systems are presented. In particular, the key concepts of distributed and decentralized ML with emphasis on federated learning (FL), serverless computing, blockchain technology, subnetworks, and device-to-device communications are discussed. In Section 3, indicative use cases are presented in the context of IEC systems, such as IoT in agriculture, smart manufacturing, efficient energy management in households, smart cities, and maritime applications. In Section 4, state-of-the-art approaches in IEC continuum systems are presented. In Section 5, a discussion based on the addressed challenges addressed by the presented work takes place. In the same context, limitations and open issues are also identified. Concluding remarks are outlined in Section 6. For the sake of illustration, an overview of the survey paper is also depicted in Figure 2.

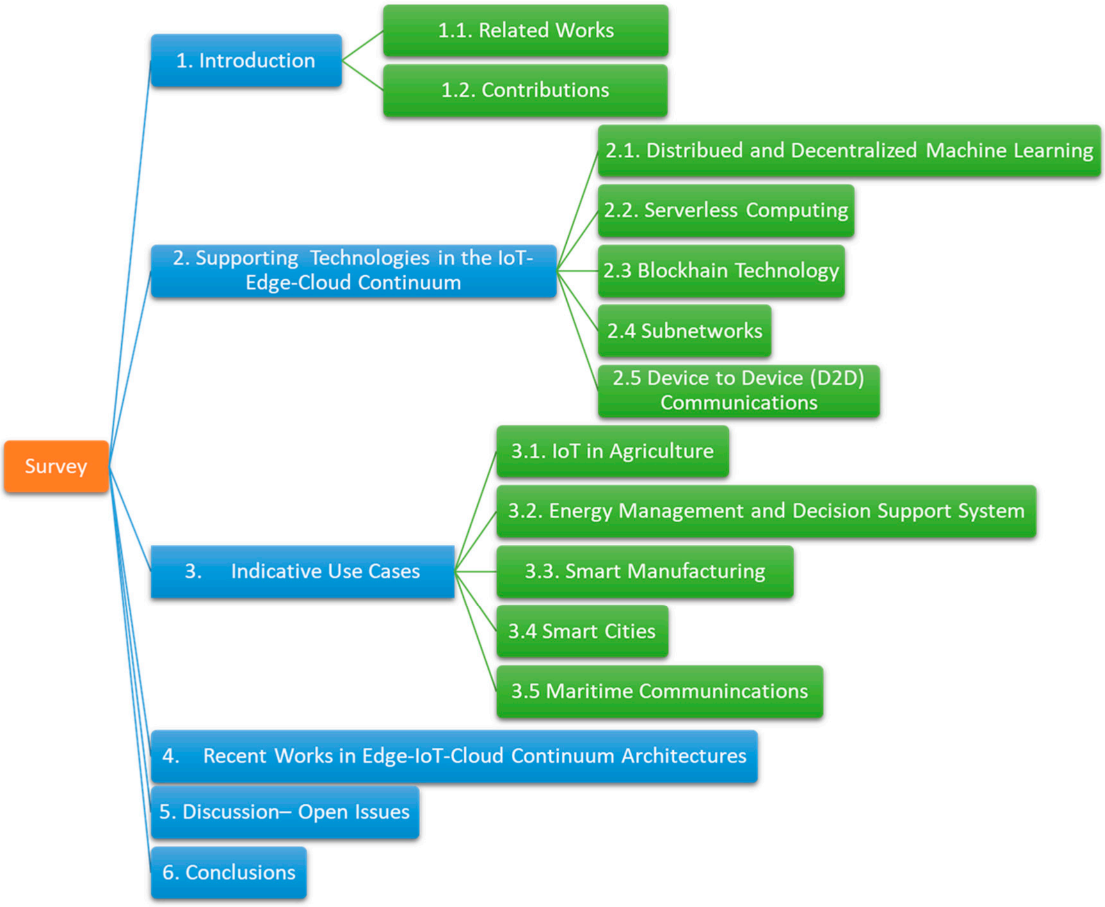
Survey
1. Introduction
1.1. Related Works
1.2. Contributions
2. Supporting Technologies in the IoT-Edge-Cloud Continuum
2.1. Distribued and Decentralized Machine Learning
2.2. Serverless Computing
2.3 Blockhain Technology
2.4 Subnetworks
2.5 Device to Device (D2D) Communications
3. Indicative Use Cases
3.1. IoT in Agriculture
3.2. Energy Management and Decision Support System
3.3. Smart Manufacturing
3.4 Smart Cities
3.5 Maritime Communincations
4. Recent Works in Edge-IoT-Cloud Continuum Architectures
5. Discussion– Open Issues
6. Conclusions

Figure 2. Survey structure.

1.1. Related Works

In this subsection, indicative recent survey papers are presented in the context of IEC systems and related fields. In [25], for example, the authors present all recent advances on edge computing-driven IoT (ECDriven IoT), which have been summarized in six main aspects: architecture of edge computing-driven IoT, operating systems, communication protocols, computing, security and privacy, as well as use cases and applications. In [26], the most important security and privacy approaches in the context of edge computing (EC)-based IoT systems are discussed. In particular, these include user-centric, device-centric, and end-to-end (E2E) security. Apart from the architectural approach per case, additional issues such as firewalls, intrusion detection systems, authentication and authorization mechanisms, and privacy-preserving designs are discussed as well. Moving a step forward, the work in [27] discusses the major classifications of attacks in IEC continuum systems and also provides possible solutions and countermeasures along with the related research efforts.

In [28], a survey of edge artificial intelligence (AI) is provided, where AI algorithms and models are deployed on edge devices. In this context, due to the resource-constraint nature of the edge devices, various technical challenges are presented and analyzed. In [29], a comprehensive survey on mobile edge computing nodes (ECNs) is presented along with related challenges and limitations. In particular, mobile ECNs are classified into four major categories, namely, aerial, ground vehicular, spatial, and maritime nodes. For each category, the different types of nodes are introduced, along with transmission and mobility limitations. A key outcome of this work is the need for an integrated architecture that takes into consideration all the aforementioned different types of nodes and diverse technical characteristics. The work in [30] is mainly focused on distributed ML approaches in the IEC continuum. In this context, the main libraries and frameworks for ML and deep learning (DL) inference, centralized training, and distributed training with a focus on the edge and cloud are presented and analyzed, along with limitations and open issues. In [31], in the context of integrating edge computing with emerging technologies in other domains (e.g., AI, blockchain, 6G, and digital twin) to support Internet of Energy (IoE) applications, the authors present an up-to-date survey of edge computing research. The research in [32] is focused on service orchestration and resource management for edge computing, including task offloading, content caching, and virtual network embedding (VNE). Finally, in [33], all recent technological advances in edge computing, especially from the perspective of architectures and models, key technologies, and directions, are presented and discussed.

The aforementioned indicative surveys are also summarized in Table 1, where the main contributions per case are highlighted. In the same context, the key contributions of our work are mentioned as well, which will be analyzed in the following subsection.

Table 1. Indicative related survey papers.

Survey Paper	Year	Contributions
[25]	2022	Edge computing-driven IoT under various technological aspects
[26]	2022	Security considerations in edge-based IoT
[27]	2021	Security and privacy considerations in IEC continuum systems and classification of attacks
[28]	2023	Edge AI
[29]	2022	Analysis of different node categories in an edge-cloud-IoT environment
[30]	2022	Frameworks and simulation tools for the support of distributed intelligence in the edge to cloud environments
[31]	2022	Integration of edge computing with novel technologies
[32]	2023	Management and orchestration in edge computing IoT systems
[33]	2022	Recent advances in edge computing
This work	-	Analysis of recent works in IEC continuum systems in the context of various challenges and key enabling technologies

1.2. Contributions

From the analysis of the previous subsection, it becomes apparent that related survey papers have dealt with a subset of the addressed challenges towards a unified IEC continuum system. For example, the works [26,27] deal with security protection and classification of attacks, while the works [28,30] deal with ML approaches. In the same context, the work [25] mainly emphasizes different architectural aspects of modern IEC approaches. Therefore, unlike other related surveys, the goal of this paper is to analyze all recent developments in the IEC continuum in the context of the addressed challenges, as described in the introductory part and also depicted in Figure 1. For this reason, the most important key enabling technologies towards an integrated IEC continuum are presented as well. This analysis is extremely important since the new era of computing systems and 6G networks will build upon a holistic integration of various cutting-edge technologies, taking into consideration, among others, the aforementioned technological challenges towards a unified access and management framework to support diverse and demanding applications. Therefore, the main contributions of our work can be summarized as follows:

- Recent works in the IEC continuum are presented, with emphasis on the challenges they deal with, as well as on the supporting technologies.
- Basic limitations are identified, and open research directions are analyzed as well. This discussion on open issues takes into consideration the coexistence of IEC systems with next-generation broadband wireless networks.
- Indicative use cases are presented, where the synergy among IoT, edge, and cloud nodes is highlighted for optimum service deployment and user experience.

2. Supporting Technologies in the IoT-Edge-Cloud Continuum

The overall architectural approach of an IEC system is shown in Figure 3 (optional communication with a 5G network has been included as well). As can be observed, various IoT nodes from different operational scenarios may communicate with 5G access points (APs) via either public or private networks. The latter case can be more appealing in latency-demanding applications, such as smart manufacturing, since all network operations can be established within the premises of interest [34,35]. It should also be noted at this point that inter-node communications can be supported as well, based on well-known communication protocols, such as Sigfox, LoRa, or narrow band (NB)-IoT [36]. It is also assumed that MEC servers can be either collocated with APs or alternately deployed in close proximity.

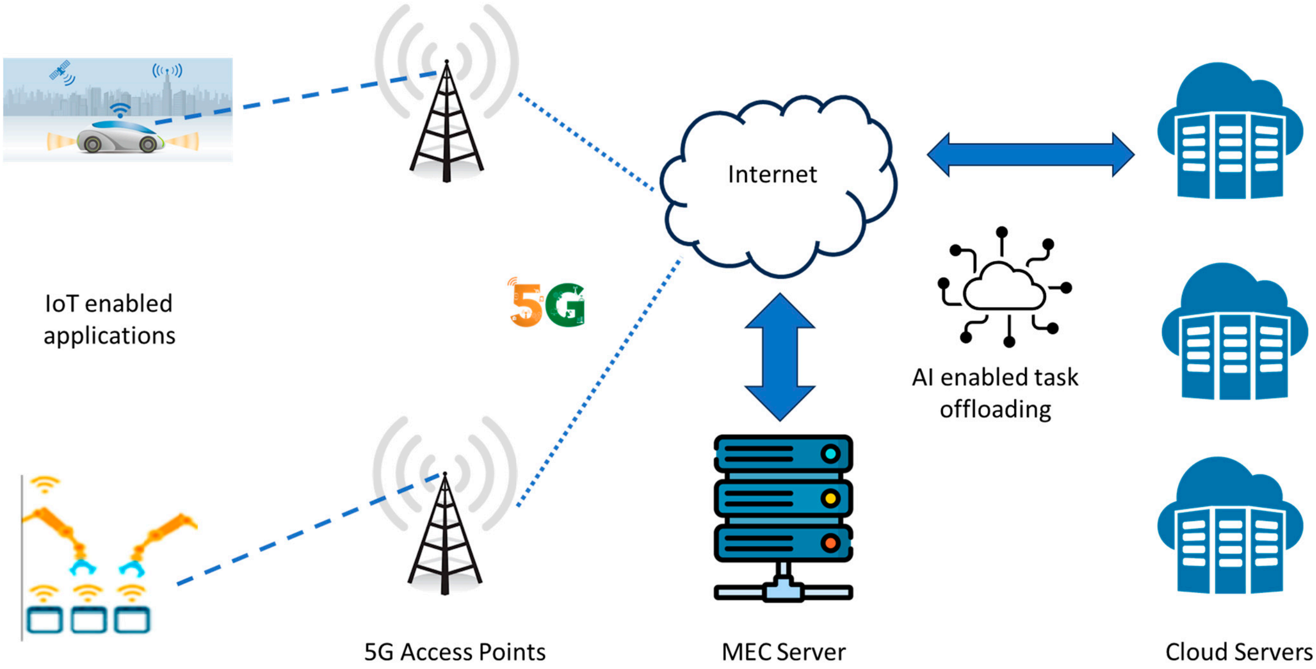

Figure 3. An IoT-edge-cloud operating system.

IoT nodes, which are assumed to have sensing and transmitting capabilities, can offload a particular task to the MEC server either in cases of latency-demanding applications or in cases of extreme computational load. This offloading may also take place in the cloud domain if necessary. In all cases, optimum task offloading should take into consideration additional parameters that may have a direct effect on the system's performance, such as the energy footprint and computational capabilities of the involved servers. Therefore, as depicted in Figure 3, efficient ML algorithms can be used for resource optimization and efficient task offloading. In all cases, it is essential to identify trusted IoT nodes and secure task offloading/data transfer procedures. Therefore, task offloading may also include the execution of advanced security protocols that might not always be feasible in resource-constraint IoT nodes. Finally, in highly demanding latency scenarios (e.g., autonomous driving in the cases of advanced 5G infrastructure [37]), the involved IoT devices should be in a position to operate autonomously and support network functionalities via NFV and ensure uninterrupted connectivity.

In light of the above, the most important key enabling technologies for an efficient IEC deployment include distributed/decentralized ML approaches for efficient resource optimization, serverless computing to leverage software and hardware decoupling, blockchain technology to ensure security during data transfer among the various nodes of the continuum as well as trusted nodes identification, subnetworks for the provision of uninterrupted connectivity, and device to device (D2D) communications for inter-node data transfer and content caching if necessary.

2.1. Distributed and Decentralized Machine Learning

As also mentioned in the introductory part, over the last decade, ML algorithms have emerged as a potential solution to relax the computational burden of traditional optimization approaches and provide near-optimum solutions in highly non-convex problems [38]. In centralized ML approaches, data collected directly from different network devices (i.e., mobile terminals, access points, IoT devices, edge servers, etc.), are sent to a high-performance computing server for proper model training. Afterwards, model inference to all involved devices takes place, if necessary.

However, there are several disadvantages with this approach, especially in the modern era of IEC systems: (i) centralized data collection might lead to high computational load, especially for a large number of involved devices and associated datasets, as well as to a single point of failure; (ii) since the vision of the IEC continuum involves multiple connected heterogeneous devices over diverse infrastructures, data preprocessing prior to the actual training of the ML model is necessary, which might increase overall training time and result in system latency deterioration; (iii) frequent transmission of data from IoT devices to centralized servers might drive security and privacy concerns since not all IoT devices have the processing power to execute advanced security protocols; and (iv) computationally demanding ML training might have an impact on the energy footprint of the involved devices.

Distributed ML approaches can reduce the centralized computational burden, either by parallelizing the training procedures or by efficiently distributing training data [39,40]. The first case, which is also known as model parallelism, enables different parts of the model to be trained on different devices (e.g., certain layers of a neural network (NN) or certain neurons per layer are trained per device). In the second case, each ML node takes into account a subset of the training data. Afterwards, model aggregation takes place. Although both aforementioned approaches can improve training times and relax the computational burden, unavoidably, training data offloading still takes place. Consequently, their deployment on privacy-critical applications might be questionable.

To overcome the aforementioned issue, the concept of FL has emerged over the last years [41,42] as a promising approach that ensures distributed ML training on the one hand and privacy protection on the other hand. To this end, training is performed locally on the involved devices, with no need for forwarding training data to external servers. At predefined time intervals, the parameters of the trained model are sent to the central processing node, where the master model is periodically updated. Moreover, since training data remain localized, privacy is enhanced, as was previously mentioned. In addition, with FL, data can be distributed across many devices, which can enable the use of much larger datasets. Moreover, the amount of data transfers and the communication burden are reduced, especially in cases where the data are distributed across devices with limited connectivity or bandwidth. Finally, FL allows the model to be trained on a diverse range of data sources, which can improve its robustness and generalizability, as well as overall training times. For example, focusing on the previously mentioned autonomous driving 5G scenario, using this approach, a predefined set of identical cars can be parallelly trained on different landscapes. Results can then be aggregated and sent back to the autonomous cars in order to cover a wide range of driving reactions.

A schematic diagram of FL is shown in Figure 4, in the case of NN training. In this case, each node locally trains the corresponding ML model with the available local data set. The derived parameters (i.e., weights of the NN in the specific case) are sent periodically to the master processing node for proper model aggregation. At the next stage, the new weights of the master model are sent back to the local nodes for a model update. Apart from autonomous driving, which was previously mentioned, FL can be quite beneficial in a wide range of scenarios, such as smart manufacturing and e-health applications, where data privacy protection is of utmost importance [43]. However, since FL is based on distributed computations, several types of privacy attacks may take place, such as poisoning and backdoor attacks [44]. Hence, privacy enhancement is a crucial step towards large-scale FL deployment.

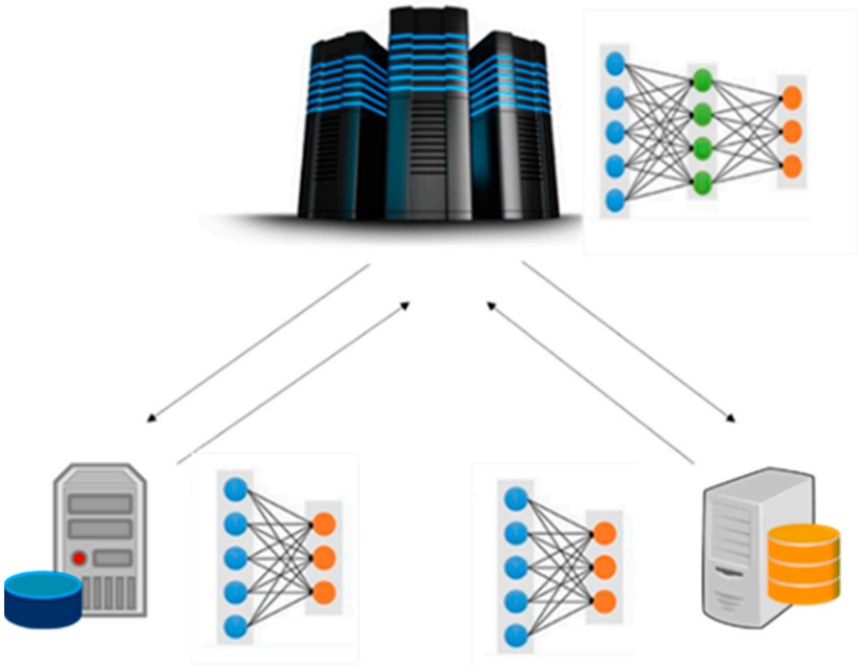

Figure 4. Federated learning in a two-node distributed system.

2.2. Serverless Computing

Serverless computing expands on state-of-the-art cloud computing by further abstracting away software operations and parts of the hardware–software stack. To this end, and with respect to the already standardized 5G architecture, the execution of vertical applications in the management and orchestration layer initiates the E2E service creation and orchestration. In the context of serverless computing [45,46], related functions need to be executed in the background for specific time triggers or generally short events. In this case, a container cluster manager (CCM) is required where the appropriate set of function containers is enabled per the requested application. Therefore, supported applications are fully decoupled from hardware infrastructure. This will not only make the support of latency-critical scenarios feasible on the one hand, such as autonomous driving, smart manufacturing, e-health applications, etc., but on the other hand, a more efficient infrastructure management can be supported.

The serverless computing concept benefits from containerization by removing decision-making regarding scaling thresholds, reducing costs by charging only when applications are triggered, and reducing application starting times. Therefore, appropriate business models can be applied in IEC continuum systems, based on the actual usage of applications. Serverless and edge computing are indispensable parts in the heterogeneous cloud environments of 6G networks, since major network functionalities should be able to migrate and be executed at the edge, either in cases of outage of the main core network or in order to leverage flexible network deployment for ultra-low latency applications.

2.3. Blockchain Technology

The ever-increasing number of interconnected devices on the Internet has raised many concerns regarding security and privacy preservation, as was previously mentioned. For example, in domestic or e-health IoT scenarios, multiple attacks may take place due to the diverse nature of the involved communication protocols [47,48]. To this end, blockchain technology is a credible way to ensure security and privacy in heterogeneous infrastructures. A blockchain is a distributed ledger technology with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. These blocks are interconnected to form a chain. Therefore, for a particular block (i.e., nth block), its hash value is calculated by hashing the whole part of the n 1 block, which in turn includes the hash of the n 2 block, etc. [49,50].

A key novelty of blockchain technology is that it does not require a central authority for node identification and verification, but transactions are made on a peer-to-peer (P2P) basis. In general, blockchain is a decentralized security mechanism, where multiple copies of blocks are held in different nodes. Therefore, a tampering attempt would have to alter all blocks in all participating nodes. Moreover, since timestamps are inserted in all related blocks, it is not possible to alter the encrypted content after it has been published to the ledger, making it more trustworthy and secure as a result. In addition, timestamps are also helpful for the tracking of the generated blocks and for statistical analysis.

The integration of blockchain technology in IoT networks faces many technical challenges since the encryption and decryption process of the blocks requires computational resources that cannot always be supported by lightweight IoT devices. Recent advances in the development of "light clients" for blockchain platforms have enabled nodes to issue transactions in the blockchain network without downloading the entire blockchain [51]. Therefore, by combining blockchain with FL, IoT sensing devices can offload a portion of their data to an edge server for local model training. However, there are still open issues to be addressed, such as a common blockchain framework that can be adopted by all involved entities, which is a key concept towards scalability in large-scale networks. Blockchain is usually combined with smart contracts, stored on a blockchain, and run only when predetermined conditions are met [52,53]. Therefore, human intervention is minimized. Smart contracts do not contain legal language, terms, or agreements—only code that executes actions. Hence, the need for trusted intermediators is reduced, while at the same time, malicious and accidental exceptions are minimized.

2.4. Subnetworks

The increased number of wireless applications deployed at the network edge involving a limited number of network components, such as a sensor network in a manufacturing environment or vehicle-to-vehicle (V2V) communications, requires minimum latency with short-range transmission. To this end, the concept of subnetworks has been introduced, where a network component in the edge acts as a serving AP [54,55]. However, the concept of subnetworks extends the provision of zero latency to the connected devices, as in cases where the connection with the core network is lost. In this case, as also mentioned in the autonomous driving application, the subnetwork should be in a position to operate autonomously for the provision of uninterrupted E2E connectivity. Sub-networks will be a key driving factor towards the 6G architectural concept due to their local topology in conjunction with the specialized performance attributes required, such as extreme latency or reliability. Moreover, the concept of subnetworks is crucial for the design of energy-efficient networks, where topology reconfiguration might take place in time-varying IoT sensor networks [56].

In 6G terminology, subnetworks are also referred to as 'in-X' subnetworks, with the 'X' standing for the entity where the subnetwork is deployed, such as a production module in a smart manufacturing environment, a robot, a vehicle, a house, or even the human body in cases of wearable devices that can monitor various parameters [57]. A schematic diagram of such a network is shown in Figure 5, where data flows are categorized according to their latency requirements: low, such as in the cases of monitoring non-latency-critical key performance indicators (KPIs); medium, such as task offloading in edge servers; and high. The latter case includes, for example, control signals from the involved IoT devices in a smart manufacturing environment that necessitate immediate production termination in cases of malfunction. Therefore, the highly critical data flows are kept within the in-X subnetwork, as the tight latency requirement does not allow for external processing. For this reason, a local edge server can be in close proximity to the AP under consideration (in this case, an unmanned aerial vehicle—UAV).

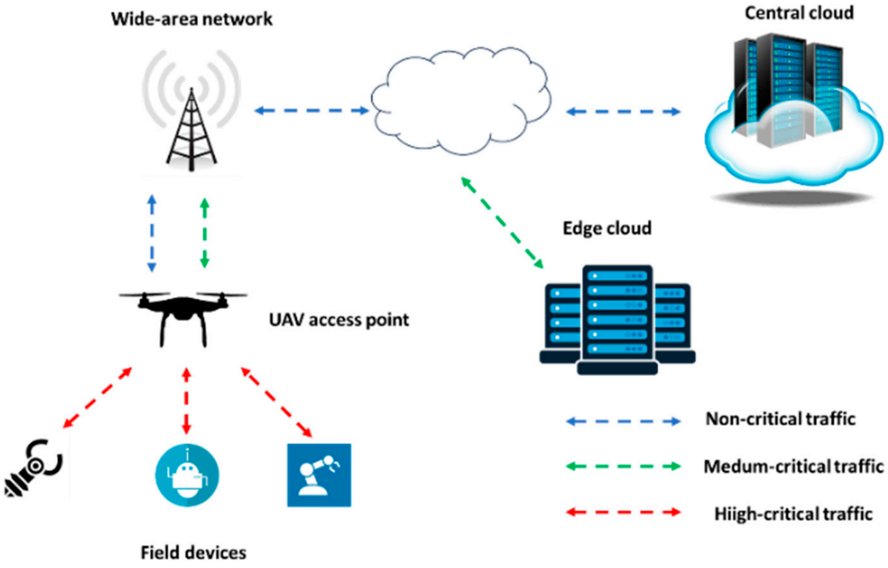

Figure 5. X subnetwork deployment within wide area networks.

2.5. Device to Device Communications

In an IoT environment, a specific type of content might be requested from several user terminals or other IoT devices in close geographical proximity. In this case, user-experienced latency can be improved if the content is requested from adjacent IoT devices that share the same content, instead of centralized APs. In this case, a particular node requests content by broadcasting a short-range signal in order to set up a link connection with the node having the content. Therefore, D2D connectivity should be supported in this case [58,59]. However, apart from content caching, D2D connectivity can also support subnetwork organization, as was mentioned in the previous subsection, as well as dynamic IoT node deployment and reconfiguration if necessary.

In general, D2D communication offers autonomous intelligent services or mechanisms without centralized supervision. Hence, the provision of ultra-low latency services in the IEC continuum can be achieved, as D2D communication offers more reliable connectivity between devices. In addition, the concept of green network deployment can be supported as well, due to the shorter propagation paths and consequently reduced transmission power.

In the same context, device interconnection can be established via mesh networking [60,61]. A mesh network comprises a type of local area network (LAN) topology, where multiple devices or nodes are connected in a non-hierarchical manner so that they can cooperate and provide significant network coverage to a wider area compared to the area coverage achieved by a single router. As mesh networks consist of multiple nodes, which are responsible for signal sending and information relaying, every node of the network needs to be connected to another via a dedicated link. Since mesh networks leverage a multi-hop wireless backbone formed by stationary routers, they can serve both mobile and stationary users. Mesh networks have significant advantages such as fast and easy network extension, self-configuration, self-healing, and reliability, as a single node failure does not result in total network failure.

3. Indicative Use Cases

In this section, indicative use cases will be presented that can be leveraged by their potential deployment in an IEC continuum environment. These use cases include IoT usage in agriculture, effective energy management coupled with a flexible decision support system, smart manufacturing in the context of Industry 4.0, smart cities, as well as maritime applications. For each use case, apart from the conceptual approach, data exchange and task offloading procedures are discussed as well.

3.1. IoT in Agriculture

Due to the large area coverage of agriculture and the variety of production objects, central cloud storage and processing of related data might significantly increase the computational load and violate latency requirements. Therefore, the IEC continuum can be beneficial for large-scale data processing and process optimization. In this context, the use of IoT devices in agriculture allows the development of processes on farms that can reduce operational costs, improve the effective use of resources, and reduce the amount of used plant protection products [62]. IoT sensor nodes can be placed in various locations of the agricultural area and measure a variety of diverse parameters, such as humidity, temperature, etc. Therefore, planting and harvesting procedures can be optimized. Other advanced applications include the usage of the so-called weeding robots that can use digital image processing to look through the images of weeds in their database to detect similarities with crops and weed out or spray them directly with their robotic arms. In the same context, harvesting robots may be used to pick crops directly from the field, thus solving the problem of labor shortages. Finally, UAVs can also be used for a variety of applications, such as high-definition two-dimensional (2D) images, weeding, etc. [63].

It becomes apparent from the above that IoT usage in agriculture can support a variety of applications with diverse requirements. These applications can be classified in terms of latency as non-critical (e.g., optimal harvesting period) as well as time-critical (e.g., field robots or UAVs on the field). In the second case, edge servers in close proximity to IoT gateways can facilitate efficient data processing via task offloading. In the same context, decision-making procedures should be expanded to a variety of field operations that include a huge amount of heterogeneous data. Therefore, decentralized ML approaches can effectively support latency/privacy critical scenarios. Finally, uninterrupted connectivity in real-time conditions and continuous monitoring of device operation when ultra-low latency is required can be supported by the concept of subnetworks, as previously mentioned. This case can be highly applicable when the agricultural field covers a wide territory and short-range network connectivity is required.

3.2. Energy Management and Decision Support System

The roll-out of smart meters around the world is part of a broader transformation in the energy sector that includes the development of smart grids, microgeneration, and the transition towards low carbon emissions. Smart meters, used to accurately measure energy consumption in households or enterprises, enable, among others, customer cost awareness, which can lead, in turn, to the shifting of energy consumption to cheaper times of the day, providing the customer with cost savings and accurate bills based on actual usage instead of estimates [64]. In addition, smart meters can measure the export of microgeneration and facilitate remuneration for electricity exported to the grid. Therefore, customers will be empowered with several advanced services and applications, such as holistic energy monitoring of their households, as well as optimum policies for buying from or selling energy to the grid. The latter case is applicable when households are equipped with renewable source generation infrastructures, such as solar panels or wind turbines, along with home battery storage. This case is also applicable when end users have electric vehicles (EVs) with bidirectional charging.

Based on the above, the provision of advanced smart services to domestic customers may include, among others, personalized and automated optimum energy usage for a household equipped with a smart meter, as well as maximization of self-consumption or minimization of carbon footprint based on household goals. Therefore, a fully deployed energy management and decision support system includes data collection from various dispersed nodes and appropriate data processing, leveraging security and privacy policies at the same time. Hence, an IEC continuum infrastructure can effectively address the aforementioned challenges. Since groups of smart meters are connected to data aggregation points via neighborhood area networks (NANs) [65], edge servers can optimize efficient data processing and fast decision-making when required. In the same context, macroscopic data collected from wide area networks (WANs) can be offloaded to the cloud for big data analysis and network reconfiguration at a large scale.

This approach may be applied to a smart home scenario, where federated learning can be employed for energy consumption prediction in households [66]. The considered structure is also depicted in Figure 6. During training, data remain localized. Hence, on the one hand, privacy concerns are mitigated, and on the other hand, faster training times can be achieved, since each local NN in a household is trained on a different sample collection. The master model is periodically updated, and the new parameters are inferred from the participating households.

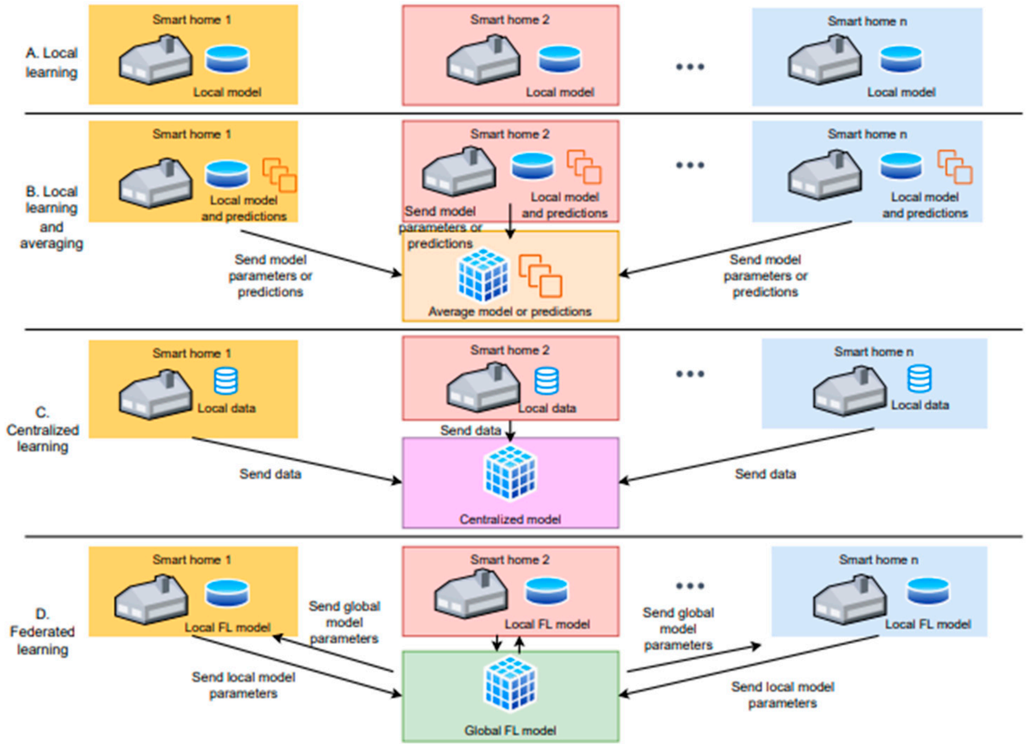

Figure 6. Federated learning in a smart-home scenario [66].

3.3. Smart Manufacturing

The IoT concept is widely applicable to industry 4.0 environments for process optimization, where sensor nodes are deployed and the collected data are offloaded to edge or cloud nodes for processing (Figure 7, [67]). In this context, the industrial Internet of Things (IIoT) is a physical network of things, objects, or devices (that contain embedded technology) for sensing and remote control in an industrial context that allows much better integration between physical and cyber worlds. To this end, there are three primary pillars that support a fully IIoT-enabled operation: (i) smart machines equipped with sensors and software that can collect and transmit various types of data; (ii) robust edge and cloud computer systems that can store and process the data; and (iii) advanced data analytics systems based on appropriate ML techniques [68,69].

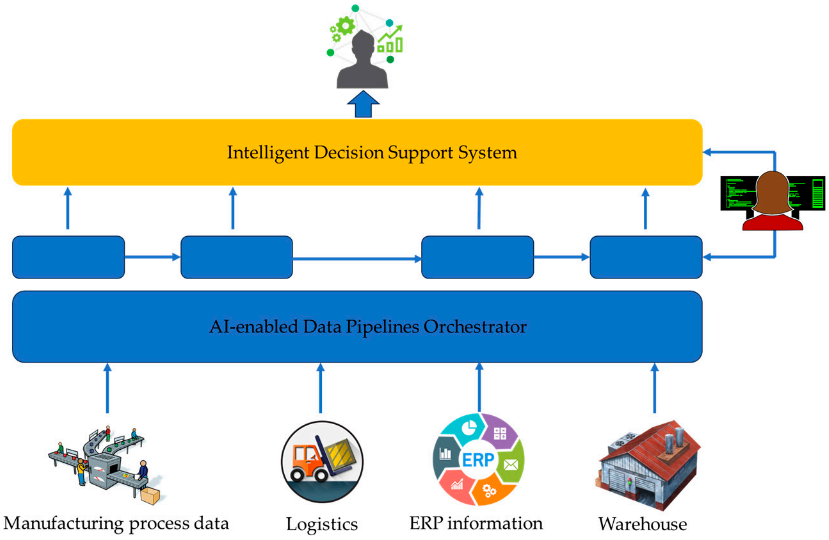
Intelligent Decision Support System
AI-enabled Data Pipelines Orchestrator
Manufacturing process data
Logistics
ERP
ERP information
Warehouse

Figure 7. Data collection and process optimization in a smart manufacturing environment [67].

Therefore, with respect to Figure 7, latency-critical tasks can be offloaded to local edge servers, and production processes can be updated accordingly. In this context, typical scenarios include failure minimization functionalities, where, for example, high-definition three-dimensional (3D) images of the products are captured by the IoT devices and compared to well-known prototypes for potential deviations.

3.4. Smart Cities

In a smart city environment, various types of data are collected and processed from different types of diverse sources: environmental monitoring, data associated with public transportation, etc. The goal is to facilitate everyday tasks and improve the quality of life of citizens. For example, end user applications can inform registered users on public transportation issues (arrivals, delays, etc.), smart traffic systems can reduce daily peaks in traffic congestion, and lighting, heating, or cooling systems can adapt their operating hours according to human presence density and thus minimize the energy footprint. All the above can be made feasible by integrating IoT technology with the edge and cloud computing [70]. Data collected directly from sensing IoT devices can be offloaded at edge servers for latency-critical applications (e.g., everyday traffic management to avoid congestion), while big data analytics can be used in the cloud infrastructure to analyze long-period time data and reconfigure infrastructure deployment if necessary.

3.5. Maritime Applications

A maritime environment is generally characterized by multiple and diverse entities dispersed over large geographical areas, including, among others, ships, vessels, ports, unmanned surface vehicles (USVs), unmanned underwater vehicles (UUVs), sensors, and actuators [71,72]. A challenging task in such a heterogeneous environment is proper data collection and processing for the optimization of various tasks related to the maritime sector, such as just-in-time arrival for vessels and ships in ports [17], pollution monitoring, search and rescue (SAR) operations, etc. Therefore, IoT devices can collect and transmit data to edge servers for proper ML training and process optimization. With respect to Figure 8, for example, a distributed ML model can be integrated into the hardware of each vessel (continuously trained with its individual operational data) and can provide recommendations for the optimized ship's speed and route planning, taking into account the time of arrival (as scheduled by the port based on the availability of its services) and the environmental weather conditions. In the same context, a centralized ML algorithm deployed at the port will indicate the optimized scheduling for the just-in-time arrival provision of port services. In this case, the cloud server collects the aggregated data and updates the corresponding models that are periodically inferred to the hardware of the vessels.

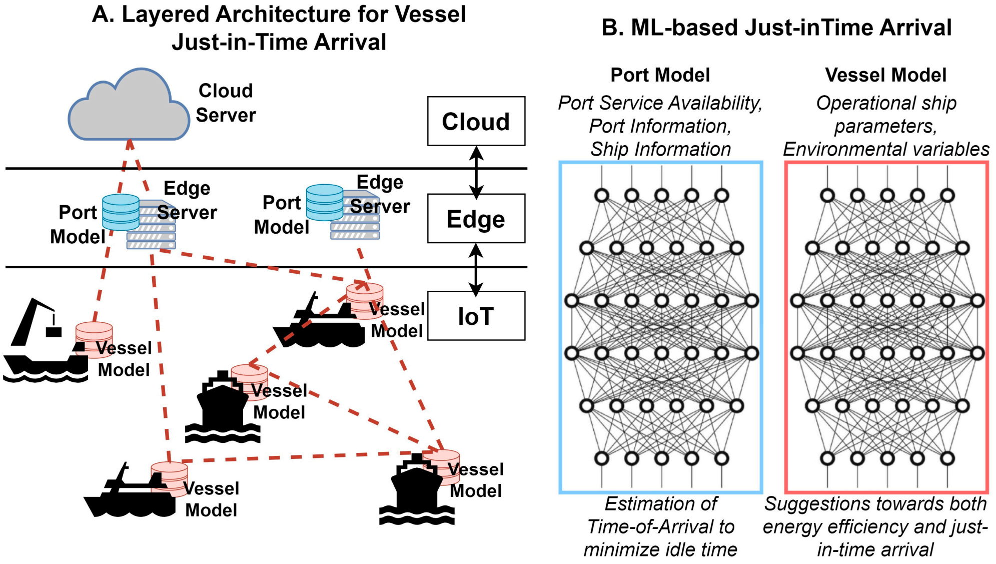
A. Layered Architecture for Vessel Just-in-Time Arrival
Cloud Server
Cloud
Edge
IoT
Port Model
Edge Server
Port Model
Edge Server
Vessel Model
Vessel Model
Vessel Model
Vessel Model
Vessel Model
B. ML-based Just-inTime Arrival
Port Model
Port Service Availability, Port Information, Ship Information
Vessel Model
Operational ship parameters, Environmental variables
Estimation of Time-of-Arrival to minimize idle time
Suggestions towards both energy efficiency and just-in-time arrival

Figure 8. IEC cloud architecture in a maritime environment for just-in-time arrival and ML model training [17].

FL can be also applicable in the maritime sector for security and privacy protection during process optimization. To this end, various critical processes can be optimized with local vessel data, such as fault diagnosis, reduction of CO_2 emissions, etc. [73,74].

4. Recent Works in IoT-Edge-Cloud Continuum Architectures

In this section, all recent advances in the area of IEC continuum systems are presented. In this context, in [75], hybrid cloud deployments for supporting data-intensive, 5G-enabled IoT applications were investigated. Moreover, a decentralized hybrid cloud MEC architecture, resulting in a Platform-as-a-Service (PaaS) is proposed and its main building blocks and layers are thoroughly described. In this context, a security and privacy module makes anomaly detection, anonymization, encryption, and identity management feasible. In addition, serverless computing is supported along with AI optimization. Moreover, two indicative use cases are provided, in particular a smart city scenario as well as e-health applications. Due to the PaaS deployment of the proposed architecture, potential stakeholders and business models are identified as well. In [76], an IEC framework is proposed and evaluated for the visual control of IoT devices in a user's smartphone. This approach couples various technologies for DNS naming and indoor localization to support the visual control of IoT devices. To this end, the DNS Name Autoconfiguration (DNSNA) for IoT devices is used, where an IoT device is registered to a router that sends a broadcast message. Afterwards, a unique DNS name and IPv6 address are generated for the specific IoT device. Localization is based on periodic WiFi beacon messages from the smartphone and the received signal strength indicator (RSSI) value for such a beacon message that is received by each IoT device. In the same context, open research challenges were identified as well, such as secure communications among the user terminal and the involved IoT devices, as well as an extension of the proposed approach in multiuser scenarios.

In [77], the UNITE architecture was described, where all available resources across the entire IEC architecture are classified into three major classes: computing, networking, and storage. To this end, holistic resource monitoring and management takes place, where the UNITE framework evaluates certain KPIs, such as latency or throughput. If one of these KPIs falls below a predefined value, then the appropriate actions take place (e.g., application migration, network rerouting, etc.) transparently to the end user. Moreover, the UNITE framework allows agnostic application development, which is not bound to any specific running environment.

In [78], an optimized IoT-enabled big data analytics architecture for edge-cloud computing using ML is proposed and evaluated. The considered scheme is composed of two layers, i.e., IoT–edge and cloud processing. In this context, an edge intelligence node is introduced, which handles and stores big amounts of data at the edges of the network with the integration of cloud technology. The proposed data design is experimentally simulated with an authentic data set using Apache Spark. In [79], the goal is to combine edge and cloud computing for IoT data analytics by taking advantage of edge nodes to reduce data transfer. In order to process data close to the source, sensors are grouped according to their locations, and feature learning is performed on the node that is closer to the edge. The results showed that transmission data and the corresponding network traffic could be reduced even up to about 80% without significant loss of accuracy. In [80], a sharing resource allocation problem among multiple service providers in the edge-cloud is investigated. In this context, the authors study distributed algorithms to find a near-optimal solution with fast convergence. In particular, the dual decomposition and alternating direction method of multipliers were used.

In [81], the concept of volunteer edge-cloud was introduced, where blockchain technology is used to deal with the problem of service payment and data credibility in a decentralized system. In this context, performance evaluation in a mobile robot environment has taken place, where a proof-of-concept system based on Ethereum and KubeEdge was designed. Results demonstrated that more flexible IoT devices can be supported, while at the same time software development is improved as well. In [82], an architectural approach is proposed and evaluated, which combines IoT, cloud, and edge computing for failure analysis and prediction. According to the presented results, the proposed model can reduce the number of failed tasks for cloud-IoT applications. In [83], a low-complexity and secure task offloading algorithm was implemented and evaluated in IEC environments. Results indicate that the proposed approach can provide a significant reduction in the overall execution times compared to other baseline approaches. In [84], the IoT microservice deployment problem is investigated in heterogeneous edge-cloud environments. In this context, microservices leverage programming flexibility, as each application can be deployed as a collection of loosely coupled services [85]. Optimum microservice deployment should take into consideration multiple applications whose execution is based on highly heterogeneous infrastructures. To this end, a deep reinforcement learning (DRL) methodology was presented in [84] that was compared with a random and a genetic algorithm. According to the presented results, the proposed approach has improved performance compared to the other benchmark approaches even when scaling up the requests.

In [86], a deep Q-learning (DQL) framework is proposed and evaluated for efficient task offloading from IoT devices to either edge or cloud servers. To this end, blockchain is used during task offloading to ensure security and privacy protection. A key novelty of this work is that it considers the energy status of each device during offloading calculations, while at the same time, an energy harvesting process is adopted per device. In [87], an IEC computing continuum solution is investigated in the context of SAR operations. These scenarios can be highly demanding both in terms of throughput and latency since they involve multiple and diverse operations, such as dynamic multi-robot mapping and fleet management, computer vision for feature extraction, data processing, device management, orchestration of software components, as well as low latency communications. The proposed approach, based on the NEPHELE project [88], leverages the virtualization of IoT devices at the edge part of the infrastructure and supports openness and interoperability aspects in a device-independent way. In the same context, an orchestration framework is supported for coordination between cloud and edge computing orchestration platforms, also considering ML and security protection.

In [89], reference architectures are discussed for industrial IoT, Internet of Vehicles (IoV) as well as IoT-based smart homes. In [90], a novel approach is introduced that adopts fuzzy logic algorithms, considering application characteristics (e.g., CPU demand, network demand, and delay sensitivity) as well as resource utilization and resource heterogeneity. The presented results indicate that this approach improves overall service time when compared to other benchmark approaches. In [91], an industrial edge-cloud collaborative computing platform is presented, namely, the Sophon Edge, which also makes use of AI-enabled operations. Sophon Edge adopts a pipeline-based computing model for streaming data from IoT devices. Moreover, this platform supports an iterative way for model evolution and updating to enable agile and data-driven IoT applications. In [92], an edge-cloud collaboration in the context of AI-assisted approaches is investigated. To this end, various aspects are discussed, such as privacy enhancement via federated learning, ML model training in hardware constraint devices, model compression, inference policies, etc. In [93], an architectural approach is presented for the IEC continuum able to be federated so as to support cross-domain services that use different cloud-IoT resources. In this context, various aspects are taken into consideration, such as content virtualization and cognitive management of services. In [94], optimum application deployment takes into consideration both required latency as well as overall power consumption. To this end, simulations were conducted with the help of the iFogSim [95] simulator, which demonstrates that application service quality is significantly improved and system power consumption is greatly reduced when compared with other baseline approaches.

In [96], the authors propose a new Internet of Things Edge-Cloud Federation (IoTEF) architecture for multi-cluster IoT applications. This new architecture has four layers: (i) application isolation; (ii) data transport; (iii) distributed operating system (OS); and (iv) unified federated management layer. This approach provides a common framework for data management to both edge and cloud, reduced latency, since data processing is closer to the edge, as well as a unified federated management approach for managing several clusters from a single management interface. In the same context, experimental results were provided as well, taking into consideration a smart building scenario. In [97], quality of service (QoS) is considered to be the main performance metric to solve the problem of optimum cluster usage in edge-cloud environments. In [98], a model-based approach to automatically assign multiple software deployment plans to hundreds of edge gateways and connected IoT devices implemented in collaboration with a smart healthcare application provider is described.

In [99], a precision agriculture (PA) case that covers extreme PA requirements by using automation, IoT technologies, and edge and cloud computing through virtualization is dealt with. In this context, a three-layered architectural approach has been considered, where IoT devices are located in greenhouse facilities and tasks can be offloaded to virtualized edge servers, while the cloud infrastructure deals with non-latency-critical high complexity calculations. In [100], an edge-fog-cloud architectural approach for IoT-based smart agricultural applications is introduced. In this context, an optimization problem is formulated using mixed-integer linear programming aiming to improve various KPIs, such as energy consumption, CO_2 emission, and network traffic.

In [101], an architectural approach to edge computing in IoT-based manufacturing applications is described. In this context, the role of edge computing is analyzed from four perspectives, in particular the following: edge equipment, network communication, information fusion, and cooperation with the cloud. In the same context, the architectural approach of [102] leverages edge-fog-cloud cooperation in a smart manufacturing environment. In [103], the architecture of an IoT big data ecosystem is presented and analyzed, based on a three-layer approach: edge layer, cloud layer, and application layer. In this context, an efficient task execution is carried out between the cloud and the edge layer, in the context of predictive maintenance.

In [104] edge computing is combined with blockchain technology in a smart manufacturing environment. In [105], a hybrid task offloading model is introduced, including the collaboration of cloud computing and MEC, in the context of smart cities. To this end, a distributed deep learning-driven task offloading algorithm is proposed to generate near-optimal offloading decisions over mobile devices, edge-cloud servers, and central cloud servers. According to the presented results, the proposed approach can significantly reduce the overall computational burden, when compared with other offloading schemes. In [106], a lightweight mechanism for security provision in IoT-based e-health applications is proposed and evaluated. To this end, potential nodes that can be used in the orientation are acceptable only in the case that can verify their trustiness. In this case, they render some services to the network, without fully being part of it. Their full admittance is based on the bootstrapping factor value. Therefore, attack attempts can be minimized. In [107], FL is used in order to reduce the amount of data sent to MEC servers for the processing and training of ML models. In this case, considering wearable devices on end users, local models can be derived based on the corresponding data sets. After the local FL training is completed, the e-health wearable device sends the corresponding local FL system model results to the MEC node, which aggregates the local FL system model (i.e., the global FL model) and broadcasts the updates to all e-health wearable users. In this context, D2D communications are also exploited. In [108], blockchain technology with smart contracts has been deployed to leverage data integrity and transaction fairness in e-health applications. According to the presented results, the proposed approach can resist adaptive chosen keyword attacks.

In [109], the problem of energy efficiency has been investigated in IEC orientations. In this context, the mathematical formulation leads to a convex optimization problem that has been solved with the help of a proposed iterative technique. To this end, the proposed approach outperforms other baseline technologies according to the resource allocation policies that have been considered, such as an equal computational load to all involved servers, a popularity-based and workload-aware assignment, as well as a communication-based assignment. In [110], the authors deal with anomaly detection in the IEC continuum. In particular, the inverse distance weighted algorithm and marching squares algorithm are adopted to generate the boundary of an anomaly in terms of isopleths. Afterwards, an appropriate filtering mechanism is employed at the edge networks, and related data are transmitted to the cloud for further analysis only if necessary. The performance of the proposed approach was evaluated with the help of a sensor telemetry data set, and the results showed that it can outperform other benchmark approaches. In [111], an IoT energy management system has been designed for smart city environments, leveraging DRL for energy-efficient calculations. In this context, two distinct approaches are evaluated: In the first case, IoT devices offload energy scheduling tasks to an edge server. In the second case, the edge server offloads NN calculations in the cloud domain to reduce overall computational times. Results were presented for specific communities with smart homes and edge servers.

According to the presented results, the proposed schemes can achieve low energy costs while causing lower delay, compared to traditional schemes. Finally, in [112], an IEC architecture is proposed and evaluated that integrates ML algorithms for optimum energy management in microgrids that employ distributed energy sources. In this context, edge devices are located in the boundaries of microgrids and collect various types of energy management data. Edge devices send telemetry data to a cloud-based IoT platform that is responsible for data monitoring, visualization, storage, and sharing for future planning purposes. The implementation is based on open-source software, and performance evaluation results address scalability for hundreds of prosumers. In particular, two forecasting algorithms were considered. As part of their future work, the authors have identified, among others, the employment of FL approaches, as well as the insertion of historical data in the considered algorithms via deep learning.

5. Discussion—Open Issues

The aforementioned works are also summarized in Table 2. To this end, the key considerations along with the adopted methodology per case are presented, along with open issues and limitations. As it became apparent from the previous analysis, the studied works consider specific use case scenarios, while at the same time addressing a subset of the IEC integration challenges, as described in Section 1. In the same context, additional key points can be outlined.

Table 2. Comparison of the presented studies—key considerations, limitations, and open issues.

Survey Paper	Year	Contributions	Methodology	Limitations—Open Issues
[75]	2019	Decentralized hybrid cloud MEC architecture	AI, security and privacy, serverless computing	Evaluation in real world scenarios
[76]	2023	Localization of IoT devices	DNS naming, IPv6	Secure communication and multi-user management
[77]	2022	Resources integration via virtualization	ML for resource optimization, agnostic application development	Security mechanisms, efficient task offloading
[78]	2023	Parallel data ingestion	ML for resource optimization, ensemble learning	Security mechanisms
[79]	2021	Data reduction prior to cloud processing	Feature learning	Extension of the proposed framework in additional applications
[80]	2022	Multiple edge/cloud providers	Resource allocation and sharing optimization model	Evaluation in real world scenarios
[81]	2021	Node utilization in IoT environments	Security via blockchain technology	Evaluation in real world scenarios
[82]	2022	Task failure minimization	Task offloading according to network, security, and latency requirements	Optimum task offloading for complex applications
[83]	2021	Efficient task offloading via security mechanisms	Advanced encryption standard cryptographic technique Low complexity load balancing and computation offloading	ML for efficient computational offloading
[84]	2021	IoT microservice deployment problem	Deep reinforcement learning	Load balancing in multi-cloud environment deployment strategies Decentralized training approaches for privacy enhancement
[86]	2023	Delay, job failure, computational overhead, energy consumption improvement	Deep Post-Decision State (PDS) for learning efficiency Blockchain technology during task offloading	ML in large-scale MEC orientations

Table 2. *Cont.*

Survey Paper	Year	Contributions	Methodology	Limitations—Open Issues
[87]	2023	Cloud-to-Edge-to-IoT Continuum for SAR applications	NFV, virtual objects at the edge	Advanced AI approaches and computer vision for additional post-disaster scenarios
[89]	2023	Integration of multiple use case scenarios in a common architectural approach	Reference architecture based on end-edge, net-edge, cloud-edge	Construction of a multi-tier EC-IoT architecture with one central cloud and multiple edge-clouds with unified regulation and standards
[90]	2021	Task offloading for latency minimization	Application characteristics and heterogeneity of the infrastructure	Evaluation in real world scenarios
[91]	2021	AI in edge-cloud-IoT environments	Sophon edge framework for ML model training and inference	Distributed ML for latency reduction and privacy enhancement
[92]	2023	Interaction between Cloud-IoT environments	Cognitive management of services	Evaluation in real world scenarios and security mechanisms
[93]	2016	Software in edge-cloud-IoT environments	Model-based approach to automatically assigning multiple software deployment plans to hundreds of edge gateways	Performance evaluation in additional scenarios apart from e-Health
[94]	2021	IoT application modules placement	Particle swarm optimization to acquire the best application module placement strategy	Extension in multiple IoT application services
[96]	2020	Multi-cluster IoT applications	Four-layered architecture	Extension in additional use case scenarios
[97]	2021	Optimum cluster usage	Task scheduling problem at the edge	Performance evaluation in real world scenarios
[98]	2022	Model fleet deployment	Model-based techniques	Evaluation in real worlds scenarios
[99]	2019	IoT platform based on edge and cloud computing for smart agriculture	Three-tier open-source software platform at local, edge and cloud planes.	Performance evaluation in additional farming scenarios
[100]	2021	IoT-Edge-Fog-Cloud architecture for agricultural applications	Optimization of energy consumption, CO_2 emission, and network traffic	Machine learning approaches
[101]	2018	IoT-based manufacturing	Interlayer coordination	Performance evaluation in large-scale orientations
[102,103]	2019, 2023	Smart manufacturing based on a three-layered architecture	Edge-fog-cloud cooperation Efficient task offloading	Performance evaluation in large-scale orientations
[104]	2020	IoT-based manufacturing	Edge computing with blockchain Task assignment based on particle swarm optimization	Performance evaluation in large-scale orientations
[105]	2020	IEC collaboration in smart cities	Distributed deep learning task offloading	Blockchain-based decentralized offloading scheme Metalearning in offloading decisions

Table 2. *Cont.*

Survey Paper	Year	Contributions	Methodology	Limitations—Open Issues
[106]	2019	IEC in e-health applications	Lightweight security mechanism based on trusted nodes	Scalability
[107]	2023	IEC in e-health applications	FL for data transfer reduction D2D communications	Single cell wireless sensor network scenario with one MEC server
[108]	2023	IEC in e-health applications	Blockchain and smart contacts	Efficient consensus algorithms
[109]	2023	Energy efficiency in IEC systems	Problem formulation, iterative optimization and comparison to baseline approaches	Energy prediction algorithms
[110]	2023	Anomaly detection in IEC systems	Interpolation and marching squares algorithm	Extension in additional real world scenarios
[111]	2019	Energy-efficient task offloading	Deep reinforcement learning in an IEC smart city scenario	Extension in additional real world scenarios
[112]	2021	Load forecasting in microgrids	Edge servers in microgrids, data collection, ML for load forecasting	Federated learning, transfer learning, insertion of historical data via deep learning

- In the cases of ML model training, in the majority of the studied works, such as in [79,84,106,111], DRL approaches have been considered, as they can adapt more effectively to various network deployments and reconfigurations. The alternative approaches of supervised or unsupervised learning would involve data collection from scratch and retraining that can increase the computational load and deteriorate the system's latency.
- The full deployment of highly demanding latency applications, such as autonomous driving or zero touch smart manufacturing, could be leveraged by private IEC infrastructures to avoid an imbalance in the computational load of edge or cloud servers from other applications and public networks' latency. In this case, private 5G infrastructures can be deployed within the premises of a manufacturing unit along with dedicated edge servers that process data and train ML models. In cases of dispersed units, these data can be then sent to private cloud domains for further analysis and macroscopic KPI optimization.
- There is a fundamental tradeoff between the enforcement of strict security policies in every data transfer procedure between IoT nodes and edge-cloud/servers and computational load. In these cases, the concept of trusted nodes can be applied: IoT nodes enter the IEC only after their robustness against specific security attacks has been verified. Even so, this does not rule out the possibility of future attacks. Therefore, anomaly detection algorithms in the edge or cloud domain can detect unusual data patterns.
- Serverless computing along with blockchain technology can be quite effective towards the concept of PaaS in IEC systems, due to the elimination of third-party involvement. By decomposing service computations as a set of microservices, service providers could make the most out of cloud and edge computing by exploiting their elasticity. During its lifetime, the service could scale-in or scale-down to adjust the number of instances of each microservice to the workload, thus reducing the operational expenditures of the service.

In the same context, as derived from the presented works, there are still open issues to be addressed prior to the full deployment of the IEC continuum.

- Resource optimization is important in the IEC continuum, due to the magnitude of involved infrastructures and applications. Therefore, the employed ML models should be in a position to collect and aggregate a vast amount of heterogeneous data from diverse sources. Moreover, the developed ML models should be applicable to multiple scenarios in the IEC framework.

- Although hardware and computational complexity along with latency reduction during task execution and efficient task offloading are the main KPIs under evaluation in an IEC ecosystem, the design and development of «green» networks are extremely important in the new era of 6G communications. In this context, the mass number of interconnected devices may have a severe impact on the energy footprint, which should be taken into account during IEC design as well. In addition, ML algorithms consume more energy compared to regular algorithms due to the increasing complexity of running and training models. Therefore, the design and implementation of less complex algorithms, while maintaining the accuracy rate, is also a key challenge towards green-based architectures.
- While some recent ML research works address intelligent orchestration and control of different edge-cloud systems, there is still a lack of integrated AI solutions to optimize the edge-cloud continuum. Therefore, it is essential to integrate ML techniques at different layers of the architecture while dynamically optimizing the edge-cloud continuum software, data, and resource orchestration as a whole. A range of techniques such as federated learning for privacy, transfer learning for model reuse at the device, and different deep reinforcement learning architectures can be applicable to various optimization goals.
- The vast majority of related works consider performance evaluation of the proposed approach per case in limited orientations (e.g., laboratory evaluation or a moderate number of participating nodes). Therefore, large-scale evaluation is important not only to examine scalability issues but also to identify potential limitations when full deployment takes place.
- The full deployment of the IEC computing systems is inextricably connected with an integration of diverse hardware elements and infrastructures, thus leading not only to a highly heterogeneous environment but also to functions and features that cannot be anticipated at the time of design. The distributed, dynamic, and programmable nature of the entire IEC continuum along with the fragmentation of data as well as the need for supporting cross-platform interoperability, makes the application of security and trust fundamentally challenging. Since such systems unavoidably lead to a corresponding increase in the number and types of potential attacks, such attacks need to be predicted and anticipated with the help of AI systems.
- The IEC framework should be able to provide autonomous reconfigurability according to network conditions and user and application requirements, as well as according to other design goals such as minimization of the energy footprint, which was previously mentioned. Indeed, the requirement for increased autonomous reconfigurability is emerging due to the ever more demanding services and the impact these services have on daily human activities (e.g., e-health applications).
- Although there are many open-source frameworks for various functionalities involved in the IEC continuum, such as Apache Kafka for telemetry and data streaming [113], TensorFlow for machine learning [114], and Flower for federating learning deployment [115], there is not until now a unified open-source framework that can support scalability over large IEC infrastructures. This diversity in programming frameworks and models hinders the efficient development of the continuum solutions.

6. Conclusions

In this survey paper, all recent advances with respect to IoT-edge-cloud-based operating systems were presented and analyzed. From the derived analysis it became apparent that the full deployment of edge-cloud-IoT systems towards the new era of broadband wireless networks will face many technical challenges, such as a unified data management system that can support multiple diverse services and applications (such as e-health, smart manufacturing, smart cities, agriculture, etc.), appropriate security mechanisms, as well as optimum resource allocation that can be adapted to various conditions. Currently missing from the IEC ecosystem is an open, non-proprietary, interoperable, robust, secure, and sustainable multi-cloud and multi-edge continuum hosting solution aimed at optimizing the execution of services, especially in data-intensive applications, and able to adapt to different and adaptable strategies (e.g., execution time reduction, concurrent execution, edge processing, fog security, locality, high resource utilization, low latency, and high energy efficiency), while being scalable, extensible, and open to experimentation. This solution should be able to support various use cases and scenarios that can be leveraged by the use of IoT technology.

Since 6G standardization is still a work in progress, with an incipient but strongly growing research effort, it is the right moment to identify the overall set of services, requirements, and functions in the IoT-cloud-edge continuum for end-to-end systems management with a strong focus on practical scenarios and applications. This joint design of the IEC continuum and 6G networks will unavoidably leverage the support of advanced services and applications in the new 6G era, such as connected intelligent machines, the Internet of Senses, as well as holoportation.

Author Contributions: Conceptualization, P.G. and P.T.; methodology, P.G.; software, A.G.; validation, A.G., P.G. and X.M.-B.; formal analysis, X.M.-B.; investigation, P.G.; resources, P.G.; data curation, X.M.-B.; writing—original draft preparation, P.G.; writing—review and editing, X.M.-B.; visualization, F.D.; supervision, F.D.; project administration, F.D.; funding acquisition, P.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the project «Towards a functional continuum operating system (ICOS)» funded by the European Commission (Project code/Grant Number: 101070177, call for proposal: HORIZON-CL4-2021-DATA-01, funded under HE | HORIZON-RIA\HORIZON-AG). For the UPC author, this work has been also partially supported by the Spanish Ministry of Science and Innovation under grant PID2021-124463OB-I00, which is funded by MCIN/AEI/10.13039/501100011033 and by ERDF A way of making Europe.

Data Availability Statement: Non-applicable (survey paper).

Conflicts of Interest: Francesco D'Andria is an employee of Eviden, BDS INN R&D (Formerly Called ATOS). The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

2D/3D	Two/Three Dimensional
5G	Fifth Generation
6G	Sixth-Generation
AI	Artificial Intelligence
AP	Access Point
CCM	Container Cluster Manager
CPU	Central Processing Unit
D2D	Device to Device
DL	Deep Learning
DRL	Deep Reinforcement Learning
DNS	Domain Name Server
DNSNA	DNS Name Autoconfiguration
DQL	Deep Q-Learning
E2E	End-to-End
EC	Edge Computing
ECN	Edge Computing Node
EV	Electrical Vehicle
FL	Federated Learning
IEC	IoT-Edge-Cloud
IioT	Industrial Internet of Things

IoE	Internet of Energy
IoT	Internet of Things
IoTEF	Internet of Things Edge-Cloud Federation
IoV	Internet of Vehicles
ECDriven IoT	Edge Computing-Driven IoT
KPI	Key Performance Indicator
LAN	Local Area Network
MEC	Multi-access Edge Computing
ML	Machine Learning
NAN	Neighborhood Area Network
NB	NarrowBand
NN	Neural Network
NFV	Network Function Virtualization
OS	Operating System
P2P	Peer to Peer
PaaS	Platform-as-a-Service
PA	Precision Agriculture
PDS	Post-Decision State
QoS	Quality of Service
RSSI	Received Signal Strength Indicator
SAR	Search and Rescue
SDN	Software Defined Networking
UAV	Unmanned Aerial Vehicle
USV/UUV	Unmanned Surface/Underwater Vehicle
V2V	Vehicle to Vehicle
VNE	Virtual Network Embedding

References

1. Masip, X.; Marín-Tordera, E.; Tashakor, G.; Jukan, A.; Ren, G.-J. Foggy clouds and cloudy fogs: A real need for coordinated management of fog-to-cloud (F2C) computing systems. *IEEE Wirel. Commun. Mag.* **2016**, *23*, 120–128. [CrossRef]
2. Pan, J.; McElhannon, J. Future edge cloud and edge computing for internet of things applications. *IEEE Internet Things J.* **2018**, *5*, 439–449. [CrossRef]
3. Zhou, I. Internet of things 2.0: Concepts, applications, and future directions. *IEEE Access* **2021**, *9*, 70961–71012. [CrossRef]
4. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J.* **2021**, *8*, 10474–10498. [CrossRef]
5. Filali, A.; Abouaomar, A.; Cherkaoui, S.; Kobbane, A.; Guizani, M. Multi-access edge computing: A Survey. *IEEE Access* **2020**, *8*, 197017–197046. [CrossRef]
6. Jiang, K.; Zhou, H.; Chen, X.; Zhang, H. Mobile edge computing for ultra-reliable and low-latency communications. *IEEE Commun. Stand. Mag.* **2021**, *5*, 68–75. [CrossRef]
7. Belcastro, L.; Marozzo, F.; Orsino, A.; Talia, D.; Trunfio, P. Edge-Cloud continuum solutions for urban mobility prediction and planning. *IEEE Access* **2023**, *11*, 38864–38874. [CrossRef]
8. Cohen, I.; Chiasserini, C.F.; Giaccone, P.; Scalosub, G. Dynamic service provisioning in the edge-cloud continuum with bounded resources. *IEEE ACM Trans. Netw.* **2023**, 1–16. [CrossRef]
9. Al-Quzweeni, A.N.; Lawey, A.Q.; Elgorashi, T.E.H.; Elmirghani, J.M.H. Optimized energy aware 5G network function virtualization. *IEEE Access* **2019**, *7*, 44939–44958. [CrossRef]
10. Cisneros, J.C.; Yangui, S.; Hernández, S.E.P.; Drira, K. A survey on distributed NFV multi-domain orchestration from an algorithmic functional perspective. *IEEE Commun. Mag.* **2022**, *60*, 60–65. [CrossRef]
11. Cox, J.H.; Chung, J.; Donovan, S.; Ivey, J.; Clark, R.J.; Riley, G.; Owen, H.L. Advancing software-defined networks: A survey. *IEEE Access* **2017**, *5*, 25487–25526. [CrossRef]
12. Raeisi-Varzaneh, M.; Dakkak, O.; Habbal, A.; Kim, B.-S. Resource scheduling in edge computing: Architecture, taxonomy, open issues and future research directions. *IEEE Access* **2023**, *11*, 25329–25350. [CrossRef]
13. Cuzzocrea, A. Effective and efficient big data management in distributed environments: Models, issues, and research perspectives. In Proceedings of the 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Larnaca, Cyprus, 14–17 May 2019; pp. 556–560. [CrossRef]
14. Samie, F.; Bauer, L.; Henkel, J. From cloud down to things: An overview of machine learning in internet of things. *IEEE Internet Things J.* **2019**, *6*, 4921–4934. [CrossRef]

15. Giannopoulos, A.; Spantideas, S.; Kapsalis, N.; Karkazis, P.; Trakadas, P. Deep reinforcement learning for energy-efficient multi-channel transmissions in 5G cognitive HetNets: Centralized, decentralized and transfer learning based solutions. *IEEE Access* **2021**, *9*, 129358–129374. [CrossRef]
16. Alsagheer, D.; Xu, L.; Shi, W. Decentralized machine learning governance: Overview, opportunities, and challenges. *IEEE Access* **2023**, *11*, 96718–96732. [CrossRef]
17. Trakadas, P.; Masip-Bruin, X.; Facca, F.M.; Spantideas, S.T.; Giannopoulos, A.E.; Kapsalis, N.C.; Martins, R.; Bosani, E.; Ramon, J.; Prats, R.G.; et al. A reference architecture for cloud–edge meta-operating systems enabling cross-domain, data-intensive, ML-assisted applications: Architectural overview and key concepts. *Sensors* **2022**, *22*, 9003. [CrossRef] [PubMed]
18. Chochliouros, I.P.; Kourtis, M.A.; Xilouris, G.; Tavernier, W.; Sanchez, E.A.; Anastassova, M.; Spiliopoulou, A.S. OASEES: An Innovative scope for a DAO-based programmable swarm solution, for decentralizing AI applications close to data generation locations. In *Artificial Intelligence Applications and Innovations. AIAI 2023 IFIP WG 12.5 International Workshops*; AIAI 2023. IFIP Advances in Information and Communication Technology; Maglogiannis, I., Iliadis, L., Papaleonidas, A., Chochliouros, I., Eds.; Springer: Cham, Switzerland, 2023; Volume 677. [CrossRef]
19. Garg, S.; Kaur, K.; Kaddoum, G.; Garigipati, P.; Aujla, G.S. Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities. *IEEE Netw.* **2021**, *35*, 298–305. [CrossRef]
20. Román-Castro, R.; López, J.; Gritzalis, S. Evolution and Trends in IoT Security. *Computer* **2018**, *51*, 16–25. [CrossRef]
21. Zhao, L.; Zhou, G.; Zheng, G.; Chih-Lin, I.; You, X.; Hanzo, L. Open-source multi-access edge computing for 6G: Opportunities and challenges. *IEEE Access* **2021**, *9*, 158426–158439. [CrossRef]
22. Firouzi, F.; Jiang, S.; Chakrabarty, K.; Farahani, B.; Daneshmand, M.; Song, J.; Mankodiya, K. Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine. *IEEE Internet Things J.* **2023**, *10*, 3686–3705. [CrossRef]
23. Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access* **2020**, *8*, 147029–147044. [CrossRef]
24. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.-J.A. The roadmap to 6G: AI empowered wireless networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
25. Kong, L.; Tan, J.; Huang, J.; Chen, G.; Wang, S.; Jin, X.; Das, S.K. Edge-computing-driven internet of things: A Survey. *ACM Comput. Surv.* **2022**, *55*, 1–41. [CrossRef]
26. Fazeldehkordi, E.; Grønli, T.-M. A survey of security architectures for edge computing-based IoT. *IoT* **2022**, *3*, 332–365. [CrossRef]
27. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet Things J.* **2021**, *8*, 4004–4022. [CrossRef]
28. Singh, R.; Gill, S.S. Edge AI: A survey. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 371–392. [CrossRef]
29. Abkenar, F.S.; Ramezani, P.; Iranmanesh, S.; Murali, S.; Chulerttiyawong, D.; Wan, X.; Raad, R. A survey on mobility of edge computing networks in IoT: State-of-the-art, architectures, and challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2329–2365. [CrossRef]
30. Rosendo, D.; Costan, A.; Valduriez, P.; Antoniu, G. Distributed intelligence on the edge-to-cloud continuum: A systematic literature review. *J. Parallel Distrib. Comput.* **2022**, *166*, 71–94. [CrossRef]
31. Kong, X.; Wu, Y.; Wang, H.; Xia, F. Edge computing for internet of everything: A survey. *IEEE Internet Things J.* **2022**, *9*, 23472–23485. [CrossRef]
32. Chiang, Y.; Zhang, Y.; Luo, H.; Chen, T.-Y.; Chen, G.-H.; Chen, H.-T.; Wang, Y.-J.; Wei, H.-Y.; Chou, C.-T. Management and orchestration of edge computing for IoT: A comprehensive survey. *IEEE Internet Things J.* **2023**, *10*, 14307–14331. [CrossRef]
33. Liu, B.; Luo, Z.; Chen, H.; Li, C. A survey of state-of-the-art on edge computing: Theoretical models, technologies, directions, and development paths. *IEEE Access* **2022**, *10*, 54038–54063. [CrossRef]
34. Sarakis, L.; Trakadas, P.; Martrat, J.; Prior, S.; Trullols-Cruces, O.; Coronado, E.; Centenaro, M.; Kontopoulos, G.; Atxutegi, E.; Gkonis, P.; et al. Cost-efficient 5G non-public network roll-out: The Affordable5G approach. In Proceedings of the IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021; pp. 221–227. [CrossRef]
35. Guo, S.; Lu, B.; Wen, M.; Dang, S.; Saeed, N. Customized 5G and beyond private networks with integrated URLLC, eMBB, mMTC, and positioning for industrial verticals. *IEEE Commun. Stand.* **2022**, *6*, 52–57. [CrossRef]
36. Cheng, Y.; Zhang, H.; Huang, Y. Overview of communication protocols in internet of things: Architecture, development and future trends. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 3–6 December 2018; pp. 627–630. [CrossRef]
37. Coronado, E.; Cebrián-Márquez, G.; Riggio, R. Enabling autonomous and connected vehicles at the 5G network edge. In Proceedings of the 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June—3 July 2020; pp. 350–352. [CrossRef]
38. Bartsiokas, I.A.; Gkonis, P.K.; Kaklamani, D.I.; Venieris, I.S. ML-based radio resource management in 5G and beyond networks: A Survey. *IEEE Access* **2022**, *10*, 83507–83528. [CrossRef]
39. Hu, S.; Chen, X.; Ni, W.; Hossain, E.; Wang, X. Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1458–1493. [CrossRef]

40. Marozzo, F.; Orsino, A.; Talia, D.; Trunfio, P. Edge computing solutions for distributed machine learning. In Proceedings of the IEEE Intelligent Conference on Dependable, Autonomic and Secure Computing, Intelligent Conference on Pervasive Intelligence and Computing, Intelligent Conference on Cloud and Big Data Computing, Intelligent Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 12–15 September 2022. [CrossRef]
41. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Process. Mag.* **2019**, *37*, 50–60. [CrossRef]
42. Rahman, K.J.; Ahmed, F.; Akhter, N.; Hasan, M.; Amin, R.; Aziz, K.E.; Islam, A.N. Challenges, applications and design aspects of federated learning: A survey. *IEEE Access* **2021**, *9*, 124682–124700. [CrossRef]
43. Ali, M.; Naeem, F.; Tariq, M.; Kaddoum, G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 778–789. [CrossRef]
44. Gosselin, R.; Vieu, L.; Loukil, F.; Benoit, A. Privacy and Security in Federated Learning: A Survey. *Appl. Sci.* **2022**, *12*, 9901. [CrossRef]
45. Li, Y.; Lin, Y.; Wang, Y.; Ye, K.; Xu, C. Serverless computing: State-of-the-art, challenges and opportunities. *IEEE Trans. Serv. Comput.* **2023**, *16*, 1522–1539. [CrossRef]
46. Patros, P.; Spillner, J.; Papadopoulos, A.V.; Varghese, B.; Rana, O.; Dustdar, S. Toward sustainable serverless computing. *IEEE Internet Comput.* **2021**, *25*, 42–50. [CrossRef]
47. Muñoz, A.; Fernández-Gago, C.; López-Villa, R. A test environment for wireless hacking in domestic IoT scenarios. In *Mobile Networks and Applications*; Springer: Berlin/Heidelberg, Germany, 2022. [CrossRef]
48. Jaime, F.J.; Muñoz, A.; Rodríguez-Gómez, F.; Jerez-Calero, A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. *Sensors* **2023**, *23*, 8944. [CrossRef] [PubMed]
49. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
50. Xu, L.D.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473. [CrossRef]
51. Shammar, E.A.; Zahary, A.T.; Al-Shargabi, A.A. A survey of IoT and blockchain integration: Security perspective. *IEEE Access* **2021**, *9*, 156114–156150. [CrossRef]
52. Kemmoe, V.Y.; Stone, W.; Kim, J.; Kim, D.; Son, J. Recent advances in smart contracts: A technical overview and state of the art. *IEEE Access* **2020**, *8*, 117782–117801. [CrossRef]
53. Abuhashim, A.; Tan, C.C. Smart contract designs on blockchain applications. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–4. [CrossRef]
54. Adeogun, R.; Berardinelli, G.; Mogensen, P.E.; Rodriguez, I.; Razzaghpour, M. Towards 6G in-X subnetworks with sub-millisecond communication cycles and extreme reliability. *IEEE Access* **2020**, *8*, 110172–110188. [CrossRef]
55. Berardinelli, G.; Adeogun, R. Hybrid radio resource management for 6G subnetwork crowds. *IEEE Commun. Mag.* **2023**, *61*, 148–154. [CrossRef]
56. Ding, Z.; Shen, L.; Chen, H.; Yan, F.; Ansari, N. Energy-efficient topology control mechanism for IoT-oriented software-defined WSNs. *IEEE Internet Things J.* **2023**, *10*, 13138–13154. [CrossRef]
57. Berardinelli, G.; Baracca, P.; Adeogun, R.O.; Khosravirad, S.R.; Schaich, F.; Upadhya, K.; Mogensen, P. Extreme communication in 6G: Vision and challenges for 'in-X' subnetworks. *IEEE OJ-COMS* **2021**, *2*, 2516–2535. [CrossRef]
58. Areqi, M.A.; Zahary, A.T.; Ali, M.N. State-of-the-art device-to-device communication solutions. *IEEE Access* **2023**, *11*, 46734–46764. [CrossRef]
59. Sarma, S.S.; Hazra, R.; Mukherjee, A. Symbiosis between D2D communication and industrial IoT for industry 5.0 in 5G mm-wave cellular network: An interference management approach. *IEEE Trans. Ind. Inform.* **2022**, *18*, 5527–5536. [CrossRef]
60. Kavitha, A.; Reddy, V.B.; Singh, N.; Gunjan, V.K.; Lakshmanna, K.; Khan, A.A.; Wechtaisong, C. Security in IoT mesh networks based on trust similarity. *IEEE Access* **2022**, *10*, 121712–121724. [CrossRef]
61. Nurlan, Z.; Kokenovna, T.Z.; Othman, M.; Adamova, A. Resource allocation approach for optimal routing in IoT wireless mesh networks. *IEEE Access* **2021**, *9*, 153926–153942. [CrossRef]
62. Zhang, X.; Cao, Z.; Dong, W. Overview of edge computing in the agricultural internet of things: Key technologies, applications, challenges. *IEEE Access* **2020**, *8*, 141748–141761. [CrossRef]
63. Moradi, S.; Bokani, A.; Hassan, J. UAV-based smart agriculture: A review of UAV sensing and applications. In Proceedings of the 32nd International Telecommunication Networks and Applications Conference (ITNAC), Wellington, New Zealand, 30 November–2 December 2022; pp. 181–184. [CrossRef]
64. Orlando, M.; Estebsari, A.; Pons, E.; Pau, M.; Quer, S.; Poncino, M.; Bottaccioli, L.; Patti, E. A smart meter infrastructure for smart grid IoT applications. *IEEE Internet Things J.* **2022**, *9*, 12529–12541. [CrossRef]
65. Alohali, B.; Kifayat, K.; Shi, Q.; Hurst, W. Group authentication scheme for neighbourhood area networks (NANs) in smart grids. *J. Sens. Actuator Netw.* **2016**, *5*, 9. [CrossRef]
66. Skianis, K.; Giannopoulos, A.; Gkonis, P.; Trakadas, P. Data aging matters: Federated learning-based consumption prediction in smart homes via age-based model weighting. *Electronics* **2023**, *12*, 3054. [CrossRef]

67. Trakadas, P.; Simoens, P.; Gkonis, P.; Sarakis, L.; Angelopoulos, A.; Ramallo-González, A.P.; Skarmeta, A.; Trochoutsos, C.; Calvo, D.; Pariente, T.; et al. An artificial intelligence-based collaboration approach in industrial IoT manufacturing: Key concepts, architectural extensions and potential applications. *Sensors* **2020**, *20*, 5480. [CrossRef]
68. Zafeiropoulos, A.; Fotopoulou, E.; Peuster, M.; Schneider, S.; Gouvas, P.; Behnke, D.; Karl, H. Benchmarking and profiling 5G verticals applications: An industrial IoT use case. In Proceedings of the 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 310–318. [CrossRef]
69. Karamplias, T.; Spantideas, S.T.; Giannopoulos, A.E.; Gkonis, P.; Kapsalis, N.; Trakadas, P. Towards closed-loop automation in 5G open RAN: Coupling an open-source simulator with xApps. In Proceedings of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Grenoble, France, 3–6 June 2022; pp. 232–237. [CrossRef]
70. Laroui, M.; Khedher, H.I.; Moungla, H.; Afifi, H.; Kamal, A.E. Virtual mobile edge computing based on IoT devices resources in smart cities. In Proceedings of the IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
71. Nomikos, N.; Gkonis, P.K.; Bithas, P.S.; Trakadas, P. A survey on UAV-aided maritime communications: Deployment considerations, applications, and future challenges. *OJ-COMS* **2023**, *4*, 56–78. [CrossRef]
72. Nomikos, N.; Giannopoulos, A.; Trakadas, P.; Karagiannidis, G.K. Uplink NOMA for UAV-aided maritime internet-of-things. In Proceedings of the 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 17–20 April 2023; pp. 1–6. [CrossRef]
73. Giannopoulos, A.; Gkonis, P.; Bithas, P.; Nomikos, N.; Ntroulias, G.; Trakadas, P. Federated Learning for Maritime Environments: Use Cases, Experimental Results, and Open Issues. Submitted for Publication in the Intelligent Transportation Systems Magazine. Available online: https://www.techrxiv.org/articles/preprint/Federated_Learning_for_Maritime_Environments_Use_Cases_Experimental_Results_and_Open_Issues/22133549/1 (accessed on 6 November 2023).
74. Giannopoulos, A.; Nomikos, N.; Ntroulias, G.; Syriopoulos, T.; Trakadas, P. Maritime Federated Learning for Decentralized On-Ship Intelligence. In *Artificial Intelligence Applications and Innovations*; AIAI 2023. IFIP Advances in Information and Communication Technology; Springer: Cham, Switzerland, 2023; Volume 676. [CrossRef]
75. Trakadas, P.; Nomikos, N.; Michailidis, E.T.; Zahariadis, T.; Facca, F.M.; Breitgand, D.; Rizou, S.; Masip, X.; Gkonis, P. Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key Issues and relevant architecture. *Sensors* **2019**, *19*, 3591. [CrossRef]
76. Ahn, Y.J.; Kim, M.; Lee, J.; Shen, Y.; Jeong, J.P. IoT edge-cloud: An internet-of-things edge-empowered cloud system for device management in smart spaces. *IEEE Netw.* **2023**. [CrossRef]
77. Brzozowski, M.; Langendoerfer, P.; Casaca, A.; Grilo, A.; Diaz, M.; Martín, C.; Camacho, J.; Landi, G. UNITE: Integrated IoT-edge-cloud continuum. In Proceedings of the IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2022; pp. 1–6. [CrossRef]
78. Babar, M. An optimized IoT-enabled big data analytics architecture for edge–cloud computing. *IEEE Internet Things J.* **2023**, *10*, 3995–4005. [CrossRef]
79. Ghosh, A.M.; Grolinger, K. Edge-cloud computing for internet of things data analytics: Embedding intelligence in the edge with deep learning. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2191–2200. [CrossRef]
80. Pham, C.; Nguyen, D.T.; Njah, Y.; Tran, N.H.; Nguyen, K.K.; Cheriet, M. Share-to-run IoT services in edge cloud computing. *IEEE Internet Things J.* **2022**, *9*, 497–509. [CrossRef]
81. Zhou, M.-T.; Shen, F.-G.; Ren, T.-F.; Feng, X.-Y. Blockchain-based volunteer edge cloud for IoT applications. In Proceedings of the IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25 April–19 May 2021. [CrossRef]
82. Jassas, M.S.; Mahmoud, Q.H. Evaluation of failure analysis of IoT applications using edge-cloud architecture. In Proceedings of the IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25–28 April 2022. [CrossRef]
83. Zhang, W.-Z.; Elgendy, I.A.; Hammad, M.; Iliyasu, A.M.; Du, X.; Guizani, M.; El-Latif, A.A.A. Secure and optimized load balancing for multitier IoT and edge-cloud computing systems. *IEEE Internet Things J.* **2021**, *8*, 8119–8132. [CrossRef]
84. Chen, L.; Xu, Y.; Lu, Z.; Wu, J.; Gai, K.; Hung, P.C.K.; Qiu, M. IoT microservice deployment in edge-cloud hybrid environment using reinforcement learning. *IEEE Internet Things J.* **2021**, *8*, 12610–12622. [CrossRef]
85. Liu, G.; Huang, B.; Liang, Z.; Qin, M.; Zhou, H.; Li, Z. Microservices: Architecture, container, and challenges. In Proceedings of the IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 11–14 December 2020; pp. 629–635. [CrossRef]
86. Heidari, A.; Navimipour, N.J.; Jamali, M.A.J.; Akbarpour, S. A green, secure, and deep intelligent method for dynamic IoT-edge-cloud offloading scenarios. *Sustain. Comput. Inform. Syst.* **2023**, *38*, 100859. [CrossRef]
87. Militano, L.; Arteaga, A.; Toffetti, G.; Mitton, N. The Cloud-to-Edge-to-IoT Continuum as an Enabler for Search and Rescue Operations. *Future Internet* **2023**, *15*, 55. [CrossRef]
88. The NEPHELE Project. Available online: https://nephele-project.eu/ (accessed on 11 July 2023).
89. Zhang, Y.; Yu, H.; Zhou, W.; Man, M. Application and Research of IoT Architecture for End-Net-Cloud Edge Computing. *Electronics* **2023**, *12*, 1. [CrossRef]
90. Almutairi, J.; Aldossary, M. A novel approach for IoT tasks offloading in edge-cloud environments. *J. Cloud Comp.* **2021**, *10*, 1–19. [CrossRef]

91. Rong, G.; Xu, Y.; Tong, X.; Fan, H. An edge-cloud collaborative computing platform for building AIoT applications efficiently. *J. Cloud Comp.* **2021**, *10*, 1–14. [CrossRef]
92. Yao, J.; Zhang, S.; Yao, Y.; Wang, F.; Ma, J.; Zhang, J.; Chu, Y.; Ji, L.; Jia, K.; Shen, T.; et al. Edge-cloud polarization and collaboration: A comprehensive survey for AI. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 6866–6886. [CrossRef]
93. Kelaidonis, D.; Rouskas, A.; Stavroulaki, V.; Demestichas, P.; Vlacheas, P. A federated edge cloud-IoT architecture. In Proceedings of the European Conference on Networks and Communications (EuCNC), Athens, Greece, 27–30 June 2016; pp. 230–234. [CrossRef]
94. Fang, J.; Ma, A. IoT application modules placement and dynamic task processing in edge-cloud computing. *IEEE Internet Things J.* **2021**, *8*, 12771–12781. [CrossRef]
95. Yousuf Khan, E.U.; Rahim Soomro, T.; Nawaz Brohi, M. iFogSim: A tool for simulating cloud and fog applications. In Proceedings of the International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022. [CrossRef]
96. Javed, A.; Robert, J.; Heljanko, K.; Främling, K. IoTEF: A federated edge-cloud architecture for fault-tolerant IoT applications. *J. Grid Computing* **2020**, *18*, 57–80. [CrossRef]
97. Mutichiro, B.; Tran, M.-N.; Kim, Y.-H. QoS-based service-time scheduling in the IoT-edge cloud. *Sensors* **2021**, *21*, 5797. [CrossRef] [PubMed]
98. Song, H.; Dautov, R.; Ferry, N.; Solberg, A.; Fleurey, F. Model-based fleet deployment in the IoT–edge–cloud continuum. *Softw. Syst. Model* **2022**, *21*, 1931–1956. [CrossRef]
99. Zamora-Izquierdo, M.A.; Santa, J.; Martínez, J.A.; Martínez, V.; Skarmeta, A.F. Smart farming IoT platform based on edge and cloud computing. *Biosyst. Eng.* **2019**, *177*, 4–17. [CrossRef]
100. Alharbi, H.A.; Aldossary, M. Energy-efficient edge-fog-cloud architecture for IoT-based smart agriculture environment. *IEEE Access* **2021**, *9*, 110480–110492. [CrossRef]
101. Chen, B.; Wan, J.; Celesti, A.; Li, D.; Abbas, H.; Zhang, Q. Edge computing in IoT-based manufacturing. *IEEE Commun. Mag.* **2018**, *56*, 103–109. [CrossRef]
102. Qi, Q.; Tao, F. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. *IEEE Access* **2019**, *7*, 86769–86777. [CrossRef]
103. Yu, W.; Liu, Y.; Dillon, T.; Rahayu, W. Edge computing-assisted IoT framework with an autoencoder for fault detection in manufacturing predictive maintenance. *IEEE Trans. Ind. Inform.* **2023**, *19*, 5701–5710. [CrossRef]
104. Lee, C.K.M.; Huo, Y.Z.; Zhang, S.Z.; Ng, K.K.H. Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology. *IEEE Access* **2020**, *8*, 28659–28667. [CrossRef]
105. Wu, H.; Zhang, Z.; Guan, C.; Wolter, K.; Xu, M. Collaborate edge and cloud computing with distributed deep learning for smart city internet of things. *IEEE Internet Things J.* **2020**, *7*, 8099–8110. [CrossRef]
106. Nwebonyi, F.N.; Martins, R.; Correia, M.E. Security and fairness in IoT based e-Health system: A case study of mobile edge-clouds. In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019; pp. 318–323. [CrossRef]
107. Hu, B.; Isaac, M.; Abdul Majeed, A.P.P.; Liu, H. Edge intelligence-based e-health wireless sensor network systems. In Proceedings of the IEEE/ACIS 23rd International Conference on Computer and Information Science (ICIS), Wuxi, China, 23–25 June 2023; pp. 55–59. [CrossRef]
108. Gao, H.; Huang, H.; Xue, L.; Xiao, F.; Li, Q. Blockchain-enabled fine-grained searchable encryption with cloud–edge computing for electronic health records sharing. *IEEE Internet Things J.* **2023**, *10*, 18414–18425. [CrossRef]
109. Xiang, Z.; Deng, S.; Zheng, Y.; Wang, D.; Tehari, J.; Zheng, Z. Energy-effective IoT services in balanced edge-cloud collaboration systems. In Proceedings of the IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 5–10 September 2021; pp. 219–229. [CrossRef]
110. Li, Y.; Zhou, Z.; Xue, X.; Zhao, D.; Hung, P.C.K. Accurate anomaly detection with energy efficiency in IoT–Edge–Cloud collaborative networks. *IEEE Internet Things J.* **2023**, *10*, 16959–16974. [CrossRef]
111. Liu, Y.; Yang, C.; Jiang, L.; Xie, S.; Zhang, Y. Intelligent edge computing for IoT-based energy management in smart cities. *IEEE Netw.* **2019**, *33*, 111–117. [CrossRef]
112. Nammouchi, A.; Aupke, P.; Kassler, A.; Theocharis, A.; Raffa, V.; Felice, M.D. Integration of AI, IoT and edge-computing for smart microgrid energy management. In Proceedings of the IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Bari, Italy, 7–10 September 2021; pp. 1–6. [CrossRef]
113. Apache Kafka. Available online: https://kafka.apache.org/ (accessed on 11 July 2023).
114. TensorFlow. Available online: https://www.tensorflow.org/ (accessed on 11 July 2023).
115. Flower, a Friendly Federated Learning Framework. Available online: https://flower.dev/ (accessed on 11 July 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.